COMPLIANCE WEEK
THE LEADING INFORMATION SERVICE ON CORPORATE GOVERNANCE, RISK, AND COMPLIANCE

The SEC's Newly Proclaimed Search Warrant Authority

John Reed Stark | January 12, 2016

John Reed Stark
Columnist

The SEC is an exceptional federal government agency—staffed with a dedicated corps of highly-credentialed professionals, inspired by a noble sense of mission, and rich with an 80+ year history of investor advocacy.

But sometimes the SEC gets carried away and needs a quick reality check. This is the case with the SEC's recent use of subpoenas demanding production from witnesses of their so-called ESDs, which stands for "electronic storage devices."

SEC ESD Subpoenas: *De Facto* Search Warrants

The SEC's authority for subpoenas is derived from Section 21 of the Securities Exchange Act of 1934, the same act that established the SEC on June 6th, of that year. The Act specifically states:

"For the purpose of any such investigation, or any other proceeding under this title, any member of the Commission or any officer designated by it, is empowered to administer oaths and affirmations, subpoena witnesses, compel their attendance, take evidence, and require the production of any books, papers, correspondence, memoranda, or other *records* which the Commission deems relevant or material to the inquiry…" (emphasis added)

The SEC staff's right to access "records" clearly contemplates something akin to a document and nowhere in any statute, rule or regulation is the staff granted authority to access physical equipment such as a file cabinet containing documents, whether that file cabinet is made of metal, wood or circuitry. This means that the SEC's subpoena for ESD is more akin to an unlawful seizure than a rightful document demand.

In addition to the questionable legality of the practice of subpoenaing devices, the risks of turning over a device to the SEC without defense counsel's proper review of that device are considerable.

First, the so-called "active data" on these devices could include irrelevant private and personal information of the user, as well as the user's friends, family, colleagues, clients, customers, etc. The devices could also include information protected by domestic or foreign statute or requiring notice of disclosure per contract. Information loaded onto the machine by another user, or privileged communications with counsel or attorney work product could also be on the machine.

Second, most users have no idea of the contents of the so-called "inactive data" on their ESDs, such as deleted recoverable files, or data located in the hard drive's unallocated space or slack space, found during a digital forensic deep dive of a hard drive.

By way of background, when a data file is deleted, its address is merely changed to unallocated space, but the text remains in free space unless it is overwritten, either intentionally or in the course of a device's normal operating processes. At the end of every saved file is "slack space", which contains various unexpected remnants, fragments and artifacts, including text from other files that were deleted then overwritten by shorter files and text that was never intentionally saved (perhaps forgotten, hidden on the device or otherwise in "not-so-plain" view). These hidden files on ESDs can include a treasure trove of inculpatory data, which a user perhaps believed had already been intentionally deleted or simply never knew existed.

> Technology has clearly transformed the investigative playing field, empowering the SEC in groundbreaking and pioneering ways to identify, pinpoint, examine, segregate, and peruse data. To its credit, when it comes to data and the ever-elusive smoking gun, the SEC has become more creative, more resourceful (and more effective) than ever.

Given the SEC's lengthy list of its Routine Uses of Information (contained in its Forms 1662 and 1661, and given to all witnesses), the SEC staff can refer any information it discovers (whether active data or inactive data) to any other investigative, prosecutorial, regulatory authority and a slew of other agencies and organizations.

What this means is that a teenage child, a family friend, or even a visiting contractor could be using a witness's computer for unlawful purposes and could have, for instance, left evidence along those lines in unallocated or slack space—and suddenly an otherwise innocent witness is arrested and carted off in handcuffs.

The SEC's "Neutral" Solution

When analyzing ESDs, the SEC digital forensics lab theoretically operates as an in-house neutral examiner, in order to advise the SEC investigatory staff with candor, veracity and transparency.

Along those lines, the SEC typically offers a compromise to witnesses who object to producing their ESDs. Specifically, the SEC offers the witness the alternative of producing their ESDs to the SEC digital forensics lab, rather than to the SEC's investigators. The lab team will then search the ESDs, and, in turn, only provide relevant, non-privileged and otherwise relevant data to the SEC investigatory team. This is a potentially foolish and dangerous arrangement for SEC witnesses.

First off, the SEC forensics team is not adequately positioned (or trained) to advocate on behalf of a witness and parse the data appropriately. Moreover, just like the SEC investigatory staff, the SEC forensic staff cannot waive the SEC's Routine Uses of Information cited above. In fact, the SEC forensics team may be lawfully required to share the witnesses' data with other law enforcement authorities, such as possible top secret or otherwise classified data; possible child pornography; or data that might relate to a crime. Once a witness produces an ESD to the government, that ESD is no longer in the witness's possession, custody or control, instead every byte of that ESD now belongs to the government.

SEC Subpoena Enforcement

SEC subpoenas are administrative subpoenas that are not self-enforcing—i.e., there is no formal avenue of objection other than to refuse to comply. Once the SEC can establish a witness's non-compliance of a subpoena, the SEC must then file a federal court case, asking a judge to order a witness to comply with that subpoena.

Yet defense counsel are loath to refuse to comply with SEC subpoenas (thus, there is a paucity case law on the subject). Why? Because refusing to comply with an SEC subpoena can:

1. Strike a perceivably uncooperative tone with the SEC staff, which can reduce the likelihood of receiving any form of cooperation credit later on;
2. Trigger a costly and injurious SEC subpoena enforcement action. Defending an SEC federal action is not only expensive, the SEC subpoena enforcement action also provides the SEC the chance to air any of its preliminary investigative findings in a public filing—which are normally kept confidential until the filing of an actual an enforcement action;
3. Prompt the SEC staff to seek a broad and sweeping asset freeze; and
4. Rile the SEC staff inadvertently, escalating the SEC's interest in a witness or creating other unintended consequences that increase unwanted, unnecessary and costly investigative scrutiny.

Criminal Investigations and ESD

Without a range of precautions, even federal criminal prosecutors do not have the authority to obtain ESDs via search warrants or to demand ESDs via subpoenas.

With respect to federal criminal search warrants for ESDs, the government must limit its searches of ESDs with the same particularity required of any search, and the government must: (1) explain how relevant data will be distinguished from irrelevant data; (2) note how the information will relate specifically to the underlying allegations; and (3) follow detailed protocols to avoid revealing non-responsive information, privileged information and other protected information. Moreover, unlike SEC subpoenas, the search warrants of federal criminal authorities are subject to judicial oversight, when the prosecutor seeks authority from a federal judge before their issuance.

Even in its own guidelines pertaining to the search and seizure of computers, the Department of Justice itself, acknowledges that the law prefers searches of all things, including computer data, to be as "discrete and specific possible," and advises federal prosecutors and agents to describe with particularity the specific set of techniques they will use to distinguish incriminating documents intermingled with innocuous ones.

With respect to federal criminal subpoenas for ESDs, the government similarly cannot avoid the probable cause and particularity requirements of a search warrant. Criminal subpoenas for devices capable of being used for data storage with no express safeguard against a subsequent rummaging through, and seizure of, irrelevant as well as relevant data (such as a judicially sanctioned search methodology), does not withstand Fourth Amendment reasonableness scrutiny.

Overbroad and Overpowered

Historically, logistical concerns, rather than legal constraints, hindered the SEC's use of overbroad subpoenas. An overbroad subpoena could result in a witnesses "backing up the truck" to SEC headquarters and dumping hundreds or even thousands of boxes of documents in response. Overbroad subpoenas before computers were a logistical nightmare, not just to review, but even to inventory, manage and warehouse, causing lengthy and tedious investigation delays.

But those days are long gone. Subpoena responses that used to require rooms, floors and buildings to store, and legions of SEC staff to review, now merely require a silicon microchip for their storage and one SEC staff member to analyze (using an e-discovery tool). Document reviews that used to take months now take hours, even minutes.

Technology has clearly transformed the investigative playing field, empowering the SEC in groundbreaking and pioneering ways to identify, pinpoint, examine, segregate, and peruse data. To its credit, when it comes to data and the ever-elusive smoking gun, the SEC has become more creative, more resourceful (and more effective) than ever.

But merely because technology facilitates the SEC's warrantless searches and seizures does not mean there exists authority to do so. During my 11-year tenure as Chief of the SEC's Office of Internet Enforcement, our office was responsible for the first, second, and third versions of the SEC's online investigative guidelines. No version of those

guidelines ever condoned the use of subpoenas for ESDs. In fact, those guidelines emphasized that for law enforcement agencies like the SEC, just because you can do something, doesn't mean you *should*.